#2

Docket No. 1046.1245

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**



In re Patent Application of:

Eiichi TAKAHASHI, et al.

Serial No.: To be Assigned

Filed: March 8, 2001

Group Art Unit: To be Assigned

Examiner: To be Assigned

For: **NETWORK SERVER LOAD DETECTION SYSTEM, SHARING SYSTEM AND METHOD**

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

*Assistant Commissioner for Patents*
*Washington, D.C. 20231*

*Sir:*

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 10-254318
Filed: September 8, 1998

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By: _____
James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

Date: 3/7/01

#2

OPB 31

# 日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　９月　８日

出願番号
Application Number: 平成１０年特許願第２５４３１８号

出願人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　２月　９日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３００６５５４

【書類名】　特許願

【整理番号】　9802512

【提出日】　平成10年 9月 8日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/56

【発明の名称】　ネットワークサーバ負荷検出装置、割当装置および方法

【請求項の数】　13

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　髙橋　英一

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　青木　武司

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　横山　乾

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　菊池　慎司

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100089244

【弁理士】

【氏名又は名称】　遠山　勉

【選任した代理人】

【識別番号】　100090516

【弁理士】

【氏名又は名称】　松倉　秀実

【連絡先】　０３－３６６９－６５７１

【手数料の表示】

【予納台帳番号】　012092

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705606

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワークサーバ負荷検出装置、割当装置および方法

【特許請求の範囲】

【請求項１】　クライアントからサーバへの通信を監視し、接続当たりの通信データサイズをサーバの負荷として計測するステップと、

接続当たりの通信データサイズの変化を検出し、最大値を記録するステップと、

前記最大値に対するその時点での接続当たりの通信データサイズが小さくなればサーバが高負荷であると判断するステップとからなるネットワークサーバ負荷検出方法。

【請求項２】　請求項１において、監視通信最小数および監視最小時間を用い、監視した通信の数が監視通信最小数に達し、かつ、計測時間が監視最小時間に達するまで、接続数および通信データサイズを計測するネットワークサーバ負荷検出方法。

【請求項３】　請求項１において、接続開始および接続終了の通信を認識し、接続開始および接続終了の通信データサイズを負荷検出対象から除外するネットワークサーバ負荷検出方法。

【請求項４】　請求項１において、接続開始通信の情報を接続終了または接続確立まで保持するステップと、

クライアントが接続失敗と判断して行う再接続のための接続開始通信を前記保持された情報に基づいて検出するステップと、

接続開始通信回数に占める再接続通信の割合をサーバの負荷とし、この割合が高い場合にサーバが高負荷であると判断するネットワークサーバ負荷検出方法。

【請求項５】　請求項１において、さらに、クライアントからの通信データサイズの分布を求めるステップと、

前記分布からサーバの負荷に関係しない極端に小さな通信データを識別するステップと、

前記極端に小さな通信データを負荷判定から除外するステップとを含むネットワークサーバ負荷検出方法。

【請求項６】　請求項１において、クライアントからサーバへの通信から少なくともシーケンス番号を求めるステップと、

前記シーケンス番号の最大値を、接続開始から終了まで保持するステップと、

受信した通信のシーケンス番号を前記で保持されたシーケンス番号と比較するステップと、

通信から得られたシーケンス番号が保持されたシーケンス番号よりも小さい場合、その通信を計測から除外するネットワークサーバ負荷検出方法。

【請求項７】　請求項１において、前記通信から得られたシーケンス番号が保持されたシーケンス番号よりも小さい場合、当該通信データを重み付け処理を行ったの後に計上する、または両シーケンス番号から経路上に問題がなかったときの通信データサイズを予測して、予測したサイズを負荷検出に計上するネットワークサーバ負荷検出方法。

【請求項８】　サーバからクライアントへの通信を監視し、サーバがクライアントへ通知する受信可能データサイズおよび接続数を計測するステップと、

接続当たりの受信可能データサイズをサーバ負荷として求めるステップと、

接続当たりの受信可能データサイズの最大値を記憶し、当該最大値に対する現接続当たりの受信可能データサイズが小さくなることでサーバが高負荷であると判断するネットワークサーバ負荷検出方法。

【請求項９】　クライアントからサーバへの通信を監視し、サーバの負荷状態を検出するサーバ負荷検出装置であって、

接続当たりの通信データのサイズを計算するデータサイズ計算手段と、

接続当たりの通信データサイズの変化を検出し、最大値を記憶する記憶手段と、

前記最大値に対するその時点での接続当たりの通信データサイズが一定値以下となったときにサーバの高負荷を検出する負荷検出手段とからなるネットワークサーバ負荷検出装置。

【請求項１０】　データをネットワークを介してクライアントから複数のサーバに転送する装置において、

クライアントから送信されるデータを宛先を変えてサーバのいずれかに転送す

る中継手段と、

データとサーバの対応関係を保持し中継手段へ宛先を指示する接続管理手段と、

サーバ、クライアントおよび経路の処理能力を計測して求め、それに基づいたサービス分配率にしたがった関数を用いてデータとサーバの対応を決定し接続管理手段へ伝えるサーバ割当手段とからなるネットワークサーバ割当装置。

【請求項１１】　前記請求項１０のサーバ割当手段において、サーバの処理能力に応じた確率分布に対し、クライアントおよび経路の処理能力が低いほど一様分布に近づける修正を行うことで求めた修正確率分布を分配率とするネットワークサーバ割当装置。

【請求項１２】

前記請求項１０のサーバ割当手段において、現在サービス中のクライアントについてのクライアントおよび経路の処理能力の分布を求め、新規接続クライアントおよび経路の処理能力が分布に対して低いほど、サーバの処理能力に応じた確率分布を一様分布に近づけ、逆に高いほど各サーバの処理能力を際立たせる修正を行い修正確率分布を求め、それを分配率とするネットワークサーバ割当装置。

【請求項１３】

前記請求項１０において、サーバ割当手段を複数有しており、当該サーバ割当手段は、クライアントやサービス毎に選択されるネットワークサーバ割当装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、サーバ資源の割り当てに関し、特に、ネットワークサービスを行うサーバへサービスを割り振る方法に関するものである。

【０００２】

【従来の技術】

近年、インターネット／イントラネットの急速な普及により、ネットワークサービスサーバの効率的利用およびサービス安定性が要求されてきている。サーバ

の効率的利用および安定したサービス供給にはサーバへのサービスの最適な割り振りが不可欠で、そのためにはサーバの負荷を正確に認識する必要がある。

【０００３】

従来技術におけるサーバの負荷認識方法としては以下に示すものが知られている。

(1).エージェント方式

サーバ上にCPUやメモリなどの資源使用率を計測するプログラムをおく方式であるが、エージェント自身がサーバの負荷を上げ、エージェントが外部と通信を行う場合、そのために帯域を消費するなど、エージェントによる負荷計測精度への干渉が生じる。また、サーバへエージェントプログラムをインストールしなければならないため、汎用性に欠け指導コストが大きいという問題があった。

(2).負荷計測通信方式

サーバに対しｐｉｎｇや擬似的なサービス通信などを行い、レスポンス時間などからサーバ負荷を求める方式であるが、計測のための通信で経路の帯域を消費してしまい、サーバも応答のための負荷を負うので負荷計測への干渉が生じる。また、計測に用いるプロトコルなどをサーバがサポートしている必要があり汎用性に欠けるといった問題があった。

(3).VC数、接続時間、接続頻度、接続エラー率、レスポンス時間の計測

これらは、クライアントからのパケットをサーバへ中継する装置上にあって、中継時に計測したサーバへのVC数、接続時間、接続頻度、接続エラー率、レスポンス時間からサーバ負荷を求める方式であるが、接続時のサーバの振る舞いに基づくため誤差が大きい。精度を上げるためには多量の接続を必要とするため、少ない接続で大量の通信を行うサービスには適さない。また、中継が必須であるため、計測装置のスループットでサーバのスループットが制限されるといった問題があった。

(4).ヒット回数、ヒット率計算方式

WWWサーバなどへのパケットを調べ、アクセス対象であるファイルなどのコンテンツ毎にアクセス回数（ヒット回数）やアクセス頻度（ヒット率）を計測し、結果からサーバ負荷を求める方式であるが、アクセス対象ファイルを特定するためにはプロトコル毎のパケット解析処理が必要になり新規サービスに対応できない。さらにサーバの性能が既知でなければならない。サーバ性能をあらかじめ与えるにはサーバ性能をカタログ値や経験で求めるしかないが、サーバ性能はシステム構成や運用形態に大きく影響されるため、標準的な構成や形態に基づいたカタログ性能値は正確でなく、経験的に求める場合は少なくとも１回の障害を避けることができないといった問題があった。

以上のように、いずれの方式もサーバに負担をかけずに高速かつ効率的にサーバの負荷を検出できるものではなかった。

【０００４】

さらに、このようなサーバの負荷が正確に認識できないために、サーバで提供されるサービスを割り振ることも難しかった。

サービスの割り振りという視点だけからは以下のような方式が提案されている。

(5).ラウンドロビンDNS方式

DNS(Domain Name System)サービスにおいて、１つのドメイン名に対し複数のサーバのIPアドレスを対応させるようエントリ表に設定しておき、クライアントからのサーバIPアドレスの問い合わせ要求に対し、各サーバをエントリ表にしたがい循環的（ラウンドロビン）に割り当て、割り当てられたサーバのIPアドレスを選択してクライアントに応えることで、サービスを複数のサーバへ分配する方式である。

【０００５】

しかし、このラウンドロビンDNS方式では、サービスの分配率は、均等であるかあるいは単純な比率でしか行えず、各サーバは、それぞれの能力や動的な負荷

状況に関係なく、割り当てられた分配率に応じてサービスを行わなければならないので、各サーバの負荷状況に差が生じてしまい、全体として非効率になってしまっていた。また、DNS問い合わせ情報は、通常クライアント側でキャッシングされてしまうので、比率変更が生じてもそれをただちに反映できないという問題もあった。

(6).ハッシュテーブルを用いた分配方式

コネクションを管理するハッシュテーブルのエントリをサーバへ割り当て、割り当てるエントリ数に応じた比率でサービスをサーバへ分配する方式である。

【０００６】

この方式ではまず、クライアントからのサービス要求時にクライアントアドレスやサービスからエントリを決め、そのエントリが割り当てられているサーバへ要求を送る。そして、割り当てたエントリ数の比率に応じた数のサービスが各サーバへ振り分けられるので、高性能サーバへ多くのエントリを割り振ったり、高負荷になったサーバへの割り当てたエントリをそれ程負荷の高くないサーバへ割り当て直したりすることでサーバの効率的利用を実現している。

【０００７】

しかし、このハッシュテーブルを用いた分配方式では、ハッシュエントリ数の比率をサービス分配率へ正しく反映させるためには、偏りのないハッシュ値を生成するハッシュ関数が必要であるが、一般にハッシュキー（クライアントアドレスやポート番号など）のあらゆる分布に対し偏りのないハッシュ値を生成するハッシュ関数を見つけることは不可能である。また、分配率の精度はハッシュエントリ数に比例するため、精度を上げるためには多数のエントリ数が必要となり、記憶資源（バッファ）を多く消費してしまう。そして、結果的にコネクション管理に使用できる記憶資源（バッファ）が少なくなってしまい、大量なアクセスを扱うことができなくなるといった問題があった。

(7).サーバの状態や性能にしたがった分配方式

サーバに対しｐｉｎｇなどでレスポンス時間を計測したり、クライアントから

のパケットを中継して、中継時に接続時間、接続エラー率などを計測してサーバの負荷の高低を予測したり、サーバ間の性能比率を予測する等して、負荷や性能比に応じた量のサービスを分配する方式である。

【０００８】

しかし、この方式では、クライアントの処理能力、クライアントまでの経路の長さや帯域幅などとは無関係にどのクライアントへのサービスも平等にサーバへ分配するため、サーバの利用効率を最大にできなかった。

【０００９】

たとえば経路の帯域幅が狭かったり長かったりして経路がボトルネックとなっているクライアントや処理能力の低いクライアントにとってサーバの性能（特にスピード）差や負荷はサービス品質には現れてこない。

【００１０】

逆に、近くや高速な回線で接続しているクライアントあるいは処理能力が高いクライアントにとってサーバの性能差や負荷はサービス品質に大きく影響することになる。そこで全てのクライアントへのサービスを平等に振り分けようとすると、クライアントにとって必要以上のサーバ資源を振り分けたり、不足したサーバ資源を振り分けたりせざるを得なくなってしまうといった問題があった。

以上述べたように、従来技術におけるサーバの負荷認識方法ならびにサーバ割当方法はいずれも問題があった。

【００１１】

本発明は、上記問題点を解決するべく提案されたものであり、その目的は、サーバの負荷をサーバに負担をかけずに高速かつ効率的に認識するとともに、サーバにおいて動的な負荷状況に応じたサービス分配を行い、設定や調整で得たサービス分配率を正確にサービス分配に反映させるとともに、クライアント毎に必要なサーバ資源を見積もりながらサービスを分配することでサーバの利用効率を最大にすることにある。

【００１２】

【課題を解決するための手段】

本発明は、前記課題を解決するため、以下の手段を採用した。

本発明の第１の手段は、クライアントからサーバへの通信を監視し、接続当たりの通信データサイズをサーバの負荷として計測するステップと、接続当たりの通信データサイズの変化を検出し、最大値を記録するステップと、前記最大値に対するその時点での接続当たりの通信データサイズが小さくなればサーバが高負荷であると判断するステップとからなるネットワークサーバ負荷検出方法である。

【００１３】

ここで、ＴＣＰ等では、サーバはクライアントから送られたパケットデータを保持するための記憶資源（バッファ）を接続毎に均等に割り当てているが、サーバは次回の受信で記憶資源（バッファ）に保持できるデータサイズをクライアントへ通知し、クライアントはサーバから通知されたサイズのデータをサーバに送るようになっている。

【００１４】

したがって、サーバが高負荷になるとクライアントから送られたデータをただちに処理できなくなるので、データの全てあるいは一部がサーバの記憶資源（バッファ）内に残留することになり、結果としてサーバは記憶資源（バッファ）内の残留データの分だけ小さいサイズをクライアントに通知せざるを得なくなる。

【００１５】

したがって、通信回線上での接続時間当たりでのデータサイズを検出することによって、サーバの高負荷状態を検出することが可能となる。

本発明の第２の手段は、前記第１の手段において、監視通信最小数および監視最小時間を用いて、監視した通信の数が監視通信最小数に達し、かつ、計測時間が監視最小時間に達するまで、接続数および通信データサイズを計測するようにした。

【００１６】

本発明の第３の手段は、前記第１の手段において、接続開始および接続終了の通信を認識し、接続開始および接続終了の通信データサイズを負荷検出対象から除外するようにした。

【００１７】

接続開始と終了の通信データは小さくサーバの負荷には依存しないので、通信総データサイズ計上から除外することで、負荷計測および高負荷判断の精度を上げる効果がある。

【００１８】

本発明の第４の手段は、前記第１の手段において、接続開始通信の情報を接続終了または接続確立まで保持するステップと、クライアントが接続失敗と判断して行う再接続のための接続開始通信を前記保持された情報に基づいて検出するステップと、接続開始通信回数に占める再接続通信の割合をサーバの負荷とし、この割合が高い場合にサーバが高負荷であると判断するものである。

【００１９】

サーバの負荷が大きい場合には、サーバはクライアントからの接続要求に応答通知を返信しなくなる。これに対してクライアントは接続要求を再送することになる。したがって、通信回線上でのクライアントの接続要求の再送を検出することによりサーバの高負荷を判定できる。

【００２０】

本発明の第５の手段は、前記第１の手段において、さらに、クライアントからの通信データサイズの分布を求めるステップと、前記分布からサーバの負荷に関係しない極端に小さな通信データを識別するステップと、前記極端に小さな通信データを負荷判定から除外するステップとを含むものである。

【００２１】

サーバ負荷に関係しない極端に小さな通信データを計測から除外することで負荷計測および高負荷検出の精度を上げる効果がある。

本発明の第６の手段は、前記第１の手段において、クライアントからサーバへの通信から少なくともシーケンス番号を求めるステップと、前記シーケンス番号の最大値を、接続開始から終了まで保持するステップと、受信した通信のシーケンス番号を前記で保持されたシーケンス番号と比較するステップと、通信から得られたシーケンス番号が保持されたシーケンス番号よりも小さい場合、その通信を計測から除外するようにした。

【００２２】

シーケンス番号は通常昇順であるが、通信回線上での輻輳などによって通信の順序性の破壊もしくは欠損が起きると順序が昇順でなくなる。サーバは到着していないデータ以降のデータを処理できないので、サーバ負荷に関わらずサーバの受信可能データサイズが小さくなり、クライアントの通信データサイズも合わせて小さくなる。経路の影響を上記の方法で回避することで、サーバ負荷計測および高負荷検出の精度を上げる効果がある。

【００２３】

本発明の第７の手段は、前記第１の手段において、前記通信から得られたシーケンス番号が保持されたシーケンス番号よりも小さい場合、当該通信データを重み付け処理を行ったの後に計上する、または両シーケンス番号から経路上に問題がなかったときの通信データサイズを予測して、予測したサイズを負荷検出に計上するようにした。

【００２４】

本発明の第８の手段は、サーバからクライアントへの通信を監視し、サーバがクライアントへ通知する受信可能データサイズおよび接続数を計測するステップと、接続当たりの受信可能データサイズをサーバ負荷として求めるステップと、接続当たりの受信可能データサイズの最大値を記憶し、当該最大値に対する現接続当たりの受信可能データサイズが小さくなることでサーバが高負荷であると判断するネットワークサーバ負荷検出方法である。

【００２５】

本発明の第９の手段は、クライアントからサーバへの通信を監視し、サーバの負荷状態を検出するサーバ負荷検出装置であって、接続当たりの通信データのサイズを計算するデータサイズ計算手段と、接続当たりの通信データサイズの変化を検出し、最大値を記憶する記憶手段と、前記最大値に対するその時点での接続当たりの通信データサイズが一定値以下となったときにサーバの高負荷を検出する負荷検出手段とからなるネットワークサーバ負荷検出装置である。

【００２６】

本発明の第１０の手段は、データをネットワークを介してクライアントから複

数のサーバに転送する装置において、クライアントから送信されるデータを宛先を変えてサーバのいずれかに転送する中継手段と、データとサーバの対応関係を保持し中継手段へ宛先を指示する接続管理手段と、サーバ、クライアントおよび経路の処理能力を計測して求め、それに基づいたサービス分配率にしたがった関数を用いてデータとサーバの対応を決定し接続管理手段へ伝えるサーバ割当手段とからなるネットワークサーバ割当装置である。

【００２７】

サーバの性能・負荷およびクライアント側の性能・負荷を計測して求めた方法にしたがってサービスを分配するので、サーバの動的な負荷状況の変化に自動的に対応でき、さらに、クライアントから見えるサービス品質を維持するために必要なだけのサーバを割り当てることができ、サーバの利用効率を最大にするという効果がある。さらに、サーバ割当決定を関数を用いて行うので、サービス分配率を正確に分配に反映できる効果がある。さらに、単一の接続管理手段のみで十分な効果を得られる。

【００２８】

本発明の第１１の手段は、前記第１０の手段でのサーバ割当手段において、サーバの処理能力に応じた確率分布に対し、クライアントおよび経路の処理能力が低いほど一様分布に近づける修正を行うことで求めた修正確率分布を分配率とするネットワークサーバ割当装置である。

【００２９】

クライアントおよび経路の処理能力の高さとサーバの処理能力がサービス品質に与える影響の大小の比例関係をサービス分配率へ反映するので、サーバ処理能力の影響がサービス品質に与える影響が大きいクライアントへ処理能力が高いサーバを優先的に割り当てることができる効果がある。

【００３０】

本発明の第１２の手段は、前記第１０の手段でのサーバ割当手段において、現在サービス中のクライアントについてのクライアントおよび経路の処理能力の分布を求め、新規接続クライアントおよび経路の処理能力が分布に対して低いほど、サーバの処理能力に応じた確率分布を一様分布に近づけ、逆に高いほど各サー

バの処理能力を際立たせる修正を行い修正確率分布を求め、それを分配率とするようにした。

【００３１】

サービス分配率を現在サービス中のクライアントおよび経路の処理能力分布との関係で調節するので、遠地からと近地からのクライアントの比率が変化するような場合でも自動的に対応できる効果がある。

【００３２】

本発明の第１３の手段は、前記第１０の手段において、サーバ割当手段を複数分であり、接続管理手段の規模はサービス分配に依存しないため、記憶資源（バッファ）の利用効率を上げる効果がある。

【００３３】

サービス別やクライアント別に割当対象サーバ群を使い分けたりサービス分配ポリシを切り替えたりするなど多様なサーバ割り当てを単一の装置で行える効果がある。

【００３４】

【発明の実施の形態】

【００３５】

【実施例１】

図１は、本実施例１におけるサーバ負荷検出装置４の機能構成を示したものである。同図に示すように、サーバ負荷検出装置４は、クライアント１とサーバ２の通信回線３に接続されており、具体的には、ルータ等に実装することも可能である。

【００３６】

このサーバ負荷検出装置４は、同図に示すように、通信回線３を伝送されるパケットデータ（ＴＣＰパケット：Transmission Control Protocol Packet）を取り込む通信データ取込部５を有している。この通信データ取込部５には、接続数検出部６、パケット数計算部８およびパケットサイズ計算部７が接続されている。

【００３７】

接続数検出部６は、通信データ取込部５が取り込んだＴＣＰパケットから単位時間当たりの接続数Ｃを検出する機能を有している。この接続数検出部６は、先頭パケットを意味するＳＹＮパケットを検出すると＋１とし、最後のパケットを意味するＦＩＮパケットを検出すると－１とする。これによって、当該サーバに現在接続されているクライアントの数が検出できることになる。

【００３８】

パケット数計算部８は、前記通信データ取込部５が取り込んだ単位時間当たりのＴＣＰパケットの数Ｎをカウントする機能を有しており、パケットサイズ計算部７は、前記通信データ取込部５が取り込んだ単位時間当たりのＴＣＰパケットの合計サイズＳを計算する機能を有している。

【００３９】

これらの各部の計算・計数データは、負荷検出部１０に送られて後述の所定の演算処理に基づいて負荷が判定される。

パケットサイズ計算部７によって計算されるパケット合計サイズＳは、計測開始時に０とし、パケットが到着したらそのパケットサイズ分だけ順次増やしていく。なお、ＳＹＮ，ＦＩＮパケットについてはデータパケットに較べてそのサイズが小さく、サーバ負荷への影響が小さいため、無視してもよい。

【００４０】

パケット数計算部８によってカウントされるパケット数Ｎは、計測開始時に０とし、パケットが到着する度に＋１とする。なお、ここでもＳＹＮ，ＦＩＮパケットについては前述した理由によりカウントを無視してもよい。

【００４１】

パケット数計算部８によるカウントはＮがある値Ｎｍｉｎを超えるまで継続するが、このＮｍｉｎを超えても計測開始からの時間があらかじめ設定された時間Ｔｍｉｎよりも短かいときには、時間Ｔｍｉｎが経過するまでカウントを継続する。

【００４２】

ここで、ＮｍｉｎおよびＴｍｉｎはあらかじめパケット数計算部８に設定して

おく。このようにＮｍｉｎ，Ｔｍｉｎを併用することで、負荷検出のためのパケットのサンプル数が少ないために生じる計算誤差を減じることができ、また、サンプル数が多すぎるために生じるオーバーフローを回避することもでき、負荷検出精度を高めることができる。

【００４３】

負荷検出部１０における負荷検出は以下の演算処理を行うことにより行われる。

まず、負荷検出部１０は、接続数検出部６から接続数Ｃを、パケットサイズ計算部７よりパケットサイズＳを受け取ると、下記の式に基づいてサーバ負荷指標値Ｌを求める。

【００４４】

なお、ここでＴはタイマ１１により計測された計測時間である。ここで設定されたＴｍｉｎ経過時にサンプルとなるカウント数ＮがＮｍｉｎを超えているときにはＴ＝Ｔｍｉｎとする。

【００４５】

$$L=(S/C)/T$$

ここで、Ｌは単位時間での１接続当たりのデータ転送量を意味することになる。このＬを用いてサーバ２の負荷を検出することができる。

【００４６】

また、負荷検出部１０では、サーバ２の処理能力限界予測値Ｌｍａｘを更新する。ここでＬｍａｘは０を初期値とし、ＬがＬｍａｘを超えた場合にはＬｍａｘの値をＬとする。ここでもし、ＬとＬｍａｘとの間に以下の関係が成立すればサーバは高負荷であると判断することができる。

$$L<\alpha Lmax \quad \text{ただし} \quad 0<\alpha<=1 \qquad \cdots (1)$$

上式（１）において、αはあらかじめ設定した定数である。

図３は、前述した負荷検出部１０における負荷検出をフロー図で示したもので

ある。

【００４７】

まず、計測が開始されると、カウント数Ｎおよびサーバ負荷指標値Ｌはリセットされ、タイマ１１がスタートされる（ステップ３０１）。そして、通信データ取込部５を介してパケットの受信が開始されると（３０２）、接続開始パケットＳＹＮであるか（３０３）、接続終了パケットＦＩＮであるか（３０５）がそれぞれ判定される。ここで、接続開始パケットＳＹＮである場合には、変数Ｖが＋１される（３０４）。また、接続終了パケットＦＩＮである場合には変数Ｖが－１される（３０６）。

【００４８】

次に、新たなパケットが受信される度にＮが＋１されてサーバ負荷指標値Ｌが負荷検出部１０で計算される（３０７）。この計算は前に説明した計算式に基づいて行われる。そして、前述の(1)式を用いて、サーバ負荷指標値Ｌがα Ｌｍａｘを超えている場合には、サーバは高負荷状態になっていると判定される。

【００４９】

このような高負荷判定は、タイマ値があらかじめ設定されたＴｍｉｎ以上となり、かつパケットのカウント数Ｎがあらかじめ設定されたＮｍｉｎ以上となったときに終了する（３０８）。

【００５０】

ここで、ＴＣＰでは、サーバ２はクライアント１から送られたパケットデータを保持するための記憶資源（バッファ）を接続毎に均等に割り当てている。サーバ２は次回の受信で記憶資源（バッファ）に保持できるデータサイズをクライアント１へ通知し、クライアント１はサーバ２から通知されたサイズのデータを通信回線３を通じてサーバ２に送るようになっている。

【００５１】

したがって、サーバ２が高負荷になるとクライアント１から送られたデータをただちに処理できなくなるので、データの全てあるいは一部がサーバ２の記憶資源（バッファ）内に残留することになり、結果としてサーバ２は記憶資源（バッファ）内の残留データの分だけ小さいサイズをクライアントに通知せざるを得な

くなる。

【００５２】

ここで、ＴＣＰはできるだけ大きなサイズのデータをやり取りするよう設計されたプロトコルであるため、サーバ２が高負荷となる前の状態では、クライアント１からサーバ２に送られるデータサイズは最大となり、その後、サーバ２の負荷が大きくなると通信回線３上を伝送されるデータサイズも小さくなる。本実施例では、図２に示すように、このデータサイズが小さくなることに着目してサーバの高負荷状態を検出している。

【００５３】

本実施例では、サーバ２が高負荷となる前の状態のときの通信回線３を伝送されるデータサイズが最大の値をＬｍａｘとしてデータベース１２に保持するようにしている。そして、(1)式で示したように、このＬｍａｘに定数αを乗じた値（しきい値）とＬとを比較し、このＬがしきい値以下となったときにサーバ２が高負荷状態であると判定している。

【００５４】

このように本実施例では、接続当たりのサイズを調べるため、接続数自体が減少することによるデータ合計サイズの減少で判断を誤ることを防ぐことができ、さらにαを用いることにより、外乱で生じるＬの変動による高負荷誤検出を防ぐことができる。

【００５５】

なお、図４のフロー図は、図３で説明したフロー図とほぼ同様であるが、通信開始パケットＳＹＮと通信終了パケットＦＩＮとを考慮しないで高負荷を判定する手順を示したものである。

【００５６】

【実施例２】

本実施例２は、クライアント１からサーバ２への再送処理を利用した高負荷検出方法である。

【００５７】

本実施例２で用いる装置構成は実施例１の図１で示したものとほぼ同様であるので図示は省略する。

本実施例２では、個々の開始パケットＳＹＮの情報をデータベース１２に記録している（図６（ａ）～（ｃ）参照）。そして、それぞれの開始パケットＳＹＮの情報は、クライアントアドレス（ＩＰ）、クライアントポート番号（ｓｐ）、サーバポート番号（ｄｐ）の組で識別するようになっている。

【００５８】

ＴＣＰではサーバ２がクライアント１からの開始パケットＳＹＮを受信すると、クライアント１に対してＳＹＮ受信確認パケットを返信する。ここで、クライアント１がサーバ２からのＳＹＮ受信確認パケットを一定時間経過しても受信できない場合、再度開始パケットＳＹＮをサーバ２に対して再送信している。

【００５９】

この概念を示したものが図５である。同図（ａ）において、まずクライアント１ａより接続要求（開始パケットＳＹＮ）がサーバ２に送信される。一方、別のクライアント１ｂからも接続要求（開始パケットＳＹＮ）がサーバ２に送信される。ここで、サーバ２のバッファ５１に余裕のある場合、すなわち低負荷状態の場合には、サーバ２は、クライアント１ａおよび１ｂに対して応答通知（受信確認パケット）を送信する。しかし、サーバ２のバッファ５１に余裕のない場合には同図（ｂ）に示すように、クライアント１からの接続要求（開始パケットＳＹＮ）に対して応答ができない。そこでクライアント１は、同図（ｃ）に示すように、一定時間内にサーバ２からの応答通知（受信確認パケット）を受領できない場合には、サーバ２に対して接続要求を再送する

本実施例２では、開始パケットＳＹＮの数Ｃｓを接続数検出部６でカウントし、クライアント１からの開始パケットＳＹＮの再送回数を検出してＣｓに対する開始パケットＳＹＮの再送回数の比率Ｒｓを算出し、これをサーバ負荷指標値Ｃｒｓとする。

【００６０】

ここで、開始パケットＳＹＮの再送は、開始パケットＳＹＮから抽出したＳＹＮ情報がデータベース１２に既に記録済みであれば再送であると判別できる。こ

のことを示したのが図６である。同図（ａ）において、負荷検出装置４のデータベースには、ＳＹＮ情報として、ＳＹＮ１（ＩＰ１，ｓｐ１，ｄｐ１）、ＳＹＮ２（ＩＰ２，ｓｐ２，ｄｐ２）およびＳＹＮ３（ＩＰ３，ｓｐ３，ｄｐ３）が記録されている。このときクライアント１からサーバに対して接続要求（開始パケットＳＹＮ４）が通信回線３を通じて発信される。負荷検出装置４は、この接続要求が、自身のデータベース１２に格納されていない接続要求、すなわち初めての接続要求である場合には、この接続要求（ＳＹＮ４：ＩＰ４，ｓｐ４，ｄｐ４）を当該データベース１２に格納する（図６（ｂ））

そして、この接続要求（ＳＹＮ４）に対してサーバ２からクライアント１に応答通知がなされないときには、クライアント１よりサーバ２に対して当該接続要求（ＳＹＮ４）が再送される。負荷検出装置４は、この接続要求（ＳＹＮ４）を通信データ取込部５で取り込んで、負荷検出部１０がデータベース１２を検索することにより、既に自身が格納している接続要求であることを知り、その結果当該接続要求（ＳＹＮ４）が再接続要求であると判定する。

【００６１】

負荷検出部１０における具体的な計測方法は実施例１で説明した接続数Ｃおよびパケットサイズｓの計数・検出方法にしたがう。

ここで、求めた開始パケットＳＹＮの再送回数の比率Ｒｓ、すなわちＣｒｓにより次式（２）が成立すればサーバ１は高負荷であると判定する。

$$Crs > \beta \quad \text{ただし、} 0 < \beta < 1 \qquad \cdots (2)$$

上式（３）において、$\beta$はあらかじめ設定された定数である。

【００６２】

サーバ２は接続毎にクライアント１からのデータを保持するバッファ５１を割り当てるが、割り当てるバッファ５１が枯渇すると接続を行わずに応答通知（ＳＹＮ受信確認パケット）をクライアント１に返さない。そのため、クライアント１は開始パケットＳＹＮの再送数の割合が増加することになる。したがって、式（２）よりサーバの高負荷を検出することが可能になる。図６（ｄ）は、このよ

うな再送率（再送回数／通信回数）とサーバ負荷の関係を示したグラフ図である。

【００６３】

なお、上式（２）の定数βは、外乱や瞬間的な高負荷状態による誤検出を防ぐためのものである。瞬間的な高負荷状態は生起確率が小さくかつ長くは続かないため、無視してよい。

【００６４】

【実施例３】

本実施例３は、負荷検出に際して、通信データサイズによって計測対象を弁別する技術である。なお、本実施例３も装置構成は図１と同様であるので、図１を用いて説明する。

【００６５】

本実施例３では、負荷検出部１０において、クライアント１からのパケットサイズＳｉとＤｓとの間に以下の関係が成立する場合はＳｉをパケット合計サイズＬに加算しないで負荷検出を行う。

$$Si < \gamma Ds \quad \cdots (3)$$

ただし、$0 < \gamma < 1$，　$Ds = f(S1, S2, \ldots, Si-1)$とする。

【００６６】

ここで、γはあらかじめ設定された定数である。Ｄｓは計測したパケットサイズの分布指標を求める関数で、たとえば平均値としてよい。またＤｓの結果値が複数の値であるならば、重み付き加算や選択などによって単一の値としてもよい。

【００６７】

ＴＣＰではクライアント１は接続後、送信データサイズをサーバ２から通知されたデータサイズよりも小さなサイズにして送信を開始し、徐々に通知データサイズまで大きくしていく。そのため接続開始後間もないクライアント１からのパ

ケットサイズはサーバ２の負荷に関わらず小さい。

【００６８】

したがって、接続開始後間もないクライアント１の数が多ければ多数の小さな送信データのために式（１）のＬを小さく見積もってしまい負荷計測、高負荷検出の精度を落としてしまう可能性がある。

【００６９】

このことを概念的に示したものが図７である。同図（ａ）では、クライアント１ａはサーバ２に対して比較的大きなサイズのパケットデータＡを送信しているが、クライアント１ｂは、通信開始後間もないため、コマンドや応答信号など、比較的小さなサイズのパケットデータＢを送信している。このような小さなパケットデータはサーバの負荷検出に際して無視して問題ない。

【００７０】

そこで、本実施例３では、式（３）を用いることにより、接続開始後間もないクライアント１からのパケットを検出してこれを計測対象から外すことで、負荷計測と高負荷検出の精度を上げている。

【００７１】

サーバが高負荷になれば、接続している全クライアントからのデータサイズが小さくなるが、データ保持のためのバッファ５１の減少は比較的緩やかであるため、上のＬの減少も緩やかである。また、全クライアントが一斉に新たに接続を開始することは確率的に低いため、式（３）で十分である。

【００７２】

精度を上げるために式（３）に適用条件としてＤｓの下限値Ｄｓｍｉｎを設定し、ＤｓがＤｓｍｉｎ以下であれば式（３）を適用しない、つまりＳｉをＬに加算するようにしてもよい。

【００７３】

【実施例４】

本実施例４は、実施例１で説明した負荷検出において、通信回線上での輻輳等により生じるパケットの矛盾によりサーバ高負荷が誤検出されてしまうことを防

止するための技術である。

【００７４】

本実施例４の装置構成は図１と同様である。ここで、クライアント１からサーバ２へのパケットは、クライアントアドレス（ＩＰ）とクライアントポート番号（ｓｐ）およびサーバポート番号（ｄｐ）の組（パケット識別子）およびシーケンス番号を接続開始から終了までがデータベース１２に保持される。このとき保持されるシーケンス番号は最大値（その時点での最終値）とする。

【００７５】

負荷検出装置４がクライアント１からのサーバ２へのパケットを受信したら、そのパケットからパケット識別子とシーケンス番号Ｐｉを求め、データベース１２に保持している同一のパケット識別子のシーケンス番号Ｐｊと比較する。

【００７６】

ここで、負荷検出部１０の判定により、Ｐｉ＜Ｐｊが成り立てば、通信回線３上でパケットの追い越しが起きたか、途中のパケットが消失したことによって再送されたことがわかる。

【００７７】

いずれにしても、このような状態でサーバ２が受け取るデータには途中で欠損が生じることになり、欠損個所以降のデータをサーバ２は処理することができず、欠損個所以降のデータはバッファ５１に残留することになる。これによりサーバ２は受信可能なデータサイズが小さくなるが、原因はサーバ負荷ではなくクライアントーサーバ間の経路での輻輳などである。

このことを概念的に示したものが図８である。同図では、クライアント１からサーバ２に対してパケットデータ「１～３」が送信されているが、これが経路輻輳等の要因でパケットデータ「２」のみが消失している。クライアント２は、受信したパケットデータ「１，３」をバッファ５１に格納する。ここで、クライアント１に対して応答通知（パケットデータ「２」の再送要求）を送るが、自身のバッファ内ではパケットデータ「２」が受信されていないため、既に到着しているパケットデータ「３」以降を処理できない状態となっている。

【００７８】

クライアント１はパケットデータ「２」に関する応答通知を重複して受信するとパケットデータ「２」の再送を行う。このようにして、パケットデータ「２～５」が揃うことによりサーバ２は受信したこれらのパケットデータを処理できる状態となるが、ただちに処理には移行できないため、クライアント１に通知するバッファの空きサイズは本来のバッファの大きさＮよりもはるかに小さいｎとなる。

【００７９】

次に、クライアント１はサーバ２から通知されたサイズｎに格納可能なサイズのパケットデータ「６」を送信するが、実際にはこのパケットデータ「６」を受信する段階では、パケットデータ「１～５」が処理されているため、バッファには広い空き空間が存在しており高負荷状態とはなっていない。

【００８０】

つまり、本実施例４では、このような図８に示した状態を高負荷と判定しないようにしている。

以上のような理由により、Ｐｉ＜Ｐｊが成立したパケットＰｉは計測から除外する。あるいはある重み付けを行い計上してもよく、さらに負荷検出部１０において、Ｐｊ－Ｐｉをパケットサイズに加えて計上してもよい。

【００８１】

ここで、Ｐｊ－Ｐｉの算出は、サーバ２内のバッファ５１に残留しているデータの予測サイズをパケットサイズに加えることでデータの欠損が生じなかった場合のサーバ２からクライアント１へ通知される受信可能データサイズすなわち現パケットのサイズの予測を行うことを意味している。

【００８２】

【実施例５】

本実施例５は、サーバ２がクライアント１に送信するパケットデータを監視することでサーバ２の負荷を判定するものである。

【００８３】

本実施例５の負荷検出装置４は、サーバ２がクライアント１へ送るパケット中

のウィンドウサイズ合計値Ｓｗと接続数Ｃとを監視する。ウィンドウサイズはサーバ２がクライアント１へ通知する受信可能なデータサイズである。

【００８４】

Ｃの値は、サーバ２からクライアント１への開始パケットＳＹＮを検出したときに１増やし、終了パケットＦＩＮを検出した場合１減じることで求める。ここで、ＳｗとＣの計測は実施例１と同様である。

【００８５】

サーバ２の負荷指標値Ｌ３は次式で求められる。Ｔは実施例１のＴと同様であるが必ずしも必須ではない。

$$L3 = (Sw / C) / T \quad \cdots (4)$$

Ｌ３は接続当たりのウィンドウサイズを意味する。Ｌ３を用いてサーバ２の高負荷を検出する方法は次の通りである。

【００８６】

まず、サーバ２の処理能力限界予測値Ｌ３ｍａｘを更新する。Ｌ３ｍａｘは、０を初期値としＬ３がＬ３ｍａｘを超えた場合にＬ３ｍａｘの値をＬ３とすることで行う。

【００８７】

ここでもし、Ｌ３とＬ３ｍａｘとの間に以下の関係が成立すれば、サーバ２は高負荷であると判定する。

$$L3 = \alpha 3 \cdot L3max \quad \text{ただし、} 0 < \alpha 3 <= 1 \quad \cdots (5)$$

上式（５）において、α3はあらかじめ設定された定数である。

【００８８】

サーバ２は、クライアント１に対して、自身が処理できるバッファ５１の空きサイズ、すなわちウィンドウサイズを通知しているが（図９（ａ））、ここで、サーバ２の負荷が上昇しクライアント１から送られたデータを完全に処理できな

くなると、図９（ｂ）に示すように、サーバ２はクライアント１に対して以前より小さいウィンドウサイズｎを通知する（より具体的には次回受信可能なデータサイズである）。このように、サーバ２からクライアントに通知されるウィンドウサイズと時間の関係をグラフで示したものが図９（ｂ）である。

【００８９】

サーバ２の負荷は接続した全てのクライアントに影響するため、Ｌ３はサーバ負荷の上昇に伴い減少する。したがって、式（４）よりサーバ負荷を計測することができ、式（５）で高負荷を検出することができる。

【００９０】

【実施例６】

本実施例６は、本発明のサーバ割当装置をクライアント・サーバ間でＴＣＰパケットを中継する装置として実現した場合である。

【００９１】

図１０において、宛先変換・パケット中継手段１００２は、クライアント１から受信したパケット１０１０が接続要求を意味する開始パケットＳＹＮであると、サービスを割り当てるサーバを決定するためにサーバ割当手段１００１のサーバ選択手段１００７に対してサーバ割当指示１０２０を出力し、クライアント側処理能力計測手段１００８に計測指示１０２１を行う。

【００９２】

サーバ処理能力計測手段１００４は、各サーバの処理能力を計算し、結果データ１０１３をサーバ割当確率計算手段１００６に送出する。各サーバの処理能力は、サーバ２に対してｐｉｎｇなどを発信してそれに対する応答時間から算出することもできるし、ユーザがあらかじめ設定しておいてもよい。また、本実施例１～５で述べたサーバ負荷検出装置を用いることもできる。

【００９３】

クライアント側処理能力計測手段１００８は、中継手段１００２からの指示があると、クライアント１および通信回線３の処理能力１０１８を計算し、サーバ割当確率修正情報生成手段１００９に報告する。ここで、クライアント側処理能

力は、たとえばクライアントに対してｐｉｎｇなどを発信してその応答時間から求めることもできる。また、Ｂｐｒｏｂなどの帯域計測手法を用いたり、クライアント１の通信についての過去の記録、パケットから抽出されるウィンドウサイズやＴＴＬから求めることもできる。

【００９４】

サーバ割当修正情報生成手段１００９は、クライアント側処理能力１０１８から、サーバ割当確率分布に対する修正関数１０２２を生成する。

図１１にサーバ割当確率分布ＰｓＤの例を、図１２下図に修正関数Ｍ（１０２２）の例を示す。

【００９５】

サーバ割当確率計算手段１００６は、サーバ割当確率分布ＰｓＤに修正関数Ｍ（１０２２）を適用してサーバ割当確率分布ＭＰｓＤを求める。

確率分布ＰｓＤは、現時点で処理能力が高いサーバほど割当確率が高くなるような分布とする。たとえば、現時点での各サーバの処理能力値（後述）をｐ１，ｐ２，．．．ｐｎ（ｎはサーバの数）とすれば、サーバＳｉへの割当確率Ｐｉを次式で求めることもできる。

$$Pi = pi / (p1 + p2 + \ldots + pn) \qquad \cdots (6)$$

確率修正関数Ｍは、図１２に示すように、クライアント側の処理能力が低いほどＰｓＤを一様分布に近づけるように修正する関数となる。たとえばｐｉｎｇなどによる応答時間Ｔｐｉｎｇをクライアント処理能力とすれば、各サーバ処理能力Ｐｉについて次の式から修正Ｐｉ’を求めてもよい。

$$Pi' = Pi + (Pav - Pi) * 2 / \pi * arc\_tan(\alpha * Tping) \qquad \cdots (7)$$

ここで、Ｐａｖは、Ｐｉの平均値であり、αはあらかじめ設定された０より大

きい数である。また、ａｒｃ＿ｔａｎ（ｘ）はｔａｎ－１（ｘ）を意味する。

【００９６】

このＰｉ’から修正確率分布ＭＰｓＤを求める。

サーバ割当確率計算手段１００６は、求めたＭＰｓＤをサーバ選択手段（１００７）に送る。サーバ選択手段（１００７）は、ＭＰｓＤから図１３に示すテーブルを生成し、０～１の任意の値をとる一様乱数値を用いて実現する。同図のテーブルは、たとえばサーバ数の要素を持つ配列で実現し、各要素に０～１までの範囲Ｐｉの最大値および最小値とサーバアドレスの組をおき、一様乱数値を含む範囲を持つ要素のサーバアドレスをサービス割当サーバアドレスとしてよい。ただし、各要素の範囲は他の要素の範囲と重複しないようにする。

【００９７】

ＰｓＤおよびＭＰｓＤの確率分布については、サーバ処理能力値ＰｉおよびＰｉ’を度数分布として実現してもよい。この場合、一様乱数値は０から全Ｐｉの合計値までの範囲をとるようにする。

【００９８】

サーバ選択手段１００７は、割当サーバを決定したらそのサーバアドレス１０１２を接続管理手段１００３に送る。

接続管理手段１００３は、宛先変換・パケット中継部より受け取った開始パケットＳＹＮまたはその一部からクライアントアドレス（ＩＰ）、クライアントポート番号（ｓｐ）、宛先ポート番号（ｄｐ）の組情報を抽出し、組情報とサーバ割当手段１００１とから受け取ったサーバアドレスの対を記録する。ここで、記録には組情報をキーとするハッシュテーブルを用いてもよい。接続管理手段１００３は、宛先変換・パケット中継手段１００２へサーバアドレス１０１２を送る。

【００９９】

宛先変換・パケット中継手段１００２は、受信したクライアント１からのパケットの宛先を接続管理手段１００３から受け取ったサーバアドレス１０１２に変換してサーバ２に送信する。

【０１００】

サービス中、宛先変換・パケット中継手段１００２は、接続管理手段１００３にパケット１０１４を送り、この接続管理手段１００３は、パケット１０１４から求めた組情報より割当サーバアドレス１０１２を求めて宛先変換・パケット中継手段１００２に送る。開始パケットＳＹＮと同様に、宛先変換・パケット中継手段１００２は、受信したクライアント１からのパケットの宛先を、接続管理手段１００３から受けたサーバアドレス１０１２に変換してサーバ２へ送信する。

【０１０１】

サービス終了時、すなわち終了パケットＦＩＮ受信時はサービス中と同様であるが、これを受信した接続管理手段１００３は、パケットに対応した組情報を破棄する。

【０１０２】

本実施例では、確率分布を用いてサービス割当を決定することで、処理能力が高いクライアントほど処理能力が高いサーバを割り当て易くなるので、応答時間などのサービス品質に対するサーバ処理能力の影響力の大小にしたがったサービス割り当てが可能になる。

【０１０３】

サーバ割当手段１００１のサーバ割当確率修正情報生成手段１００９は、過去のクライアント側処理能力の分布（図１４）を求め、新規接続クライアントのクライアント処理能力値の分布からの隔たりδを求め、新規接続クライアントのクライアント側処理能力値の分布からの隔たりδｃを求める。そしてδｃを修正関数Ｍに加味して確率分布を修正する（図１５）。ここで、たとえばδｃを以下の式で求める。

$$\delta c = Pca - pci$$

ここで、Ｐｃａは過去のクライアント側処理能力平均値であり、ｐｃｉは新規接続クライアントのクライアント側処理能力値である。δｃが小さいほどサーバ処理能力値ｐｉを全ｐｉの平均値に近づけ大きいほど平均値からの隔たりを大きくするように修正関数Ｍを定める。ただし、平均値からの隔たりを大きくする場

合、ｐｉの修正値ｐｉ’が負数にならないようにする。たとえば、式（７）を以下のようにしてもよい。

ｐｉ’＝ｐｉ＋（Ｐａｖ－ｐｉ）＊β＊２／π＊ａｒｃ＿ｔａｎ（α＊δｃ＋γ）

・・・（７’）

ここで、Ｐａｖはｐｉの平均値であり、α、γはあらかじめ設定された０より大きい数である。また、ａｒｃ＿ｔａｎ（ｘ）はｔａｎ－１（ｘ）を意味する。βは－１のとき、δｃ＜０であり、－ｄｐｊ／ｐｊのときδ＞＝０である。ｐｊはｐｉの最小値であり、ｄｐｊ＝Ｐａｖ－ｐｊとなる。

【０１０４】

このように、新規接続クライアントのクライアント側処理能力値の過去のクライアント側処理能力値の分布に対する隔たりにしたがってサーバ割当を行うことにより、各時点におけるクライアントに応じたサーバ割当が可能となる。たとえば、遠隔地からと近隣地からのクライアントの比率が時間帯によって変動する場合などに自動的に対応することが可能となる。

【０１０５】

さらに、本実施例では、サーバ割当手段（１００１）を複数配置して、それぞれをクライアントアドレス、クライアントポート番号、サービスポート番号などに応じて選択してもよい。

【０１０６】

サービス毎やクライアント毎に割当対象サーバ群を使い分けたり、サービス分配ポリシを切り替えたりすることが可能となり、多様なサービス割当を一つの装置で行うことができる。

【０１０７】

【発明の効果】

以上説明してきたように、本発明は、サーバの負荷計測および高負荷検出をクライアント・サーバ間の通信を監視して行うので、サーバへ手を加える必要がな

く、サービス以外のパケットを出さない。したがって、いかなるサーバへも対処でき導入コストが低く負荷への干渉が一切ないという効果がある。また、プロトコルに依存しない指標で負荷計測、高負荷検出を行うので、いかなるサービスへも対処できるという効果もあり、サービス中の通信状態を監視するために外乱の影響が小さく精度が高いという効果もある。

【０１０８】

さらに、サーバの提供するサービスを複数のサーバに分担させる際、サーバ構成の変更やサーバの状態の変化に対し、クライアントから見えるサービス品質に対するサーバ処理能力の影響の大小に応じて各サーバの負荷分担を自動的に、かつ、効率的に割り振るので、クライアントにとって、迅速なサービスの供給を受けることができる効果がある。

【図面の簡単な説明】

【図１】　本発明の実施形態である負荷検出装置の接続構成を示す図

【図２】　実施形態におけるサーバの高負荷判定を行うためのデータサイズと時間との関係を示したグラフ図

【図３】　実施例１におけるパケット監視方法を示すフロー図（１）

【図４】　実施例１におけるパケット監視方法を示すフロー図（２）

【図５】　クライアントからサーバへの接続要求と、バッファの状態に応じた応答処理を説明するための図

【図６】　クライアントからサーバへの接続要求の再送を説明するための図

【図７】　負荷検出においてデータサイズによって対象データとするか否かの弁別を行う例を示す説明図

【図８】　シーケンス番号に基づくサーバの処理を説明するための図

【図９】　サーバからクライアントへの通信を監視する説明図

【図１０】　実施形態のサーバ割当装置の構成を示すブロック図

【図１１】　サーバ割当確率分布ＰｓＤを説明するためのグラフ図

【図１２】　修正関数を説明するための図（１）

【図１３】　実施形態において、サーバ選択手段により生成されるテーブル

の一例を示す図

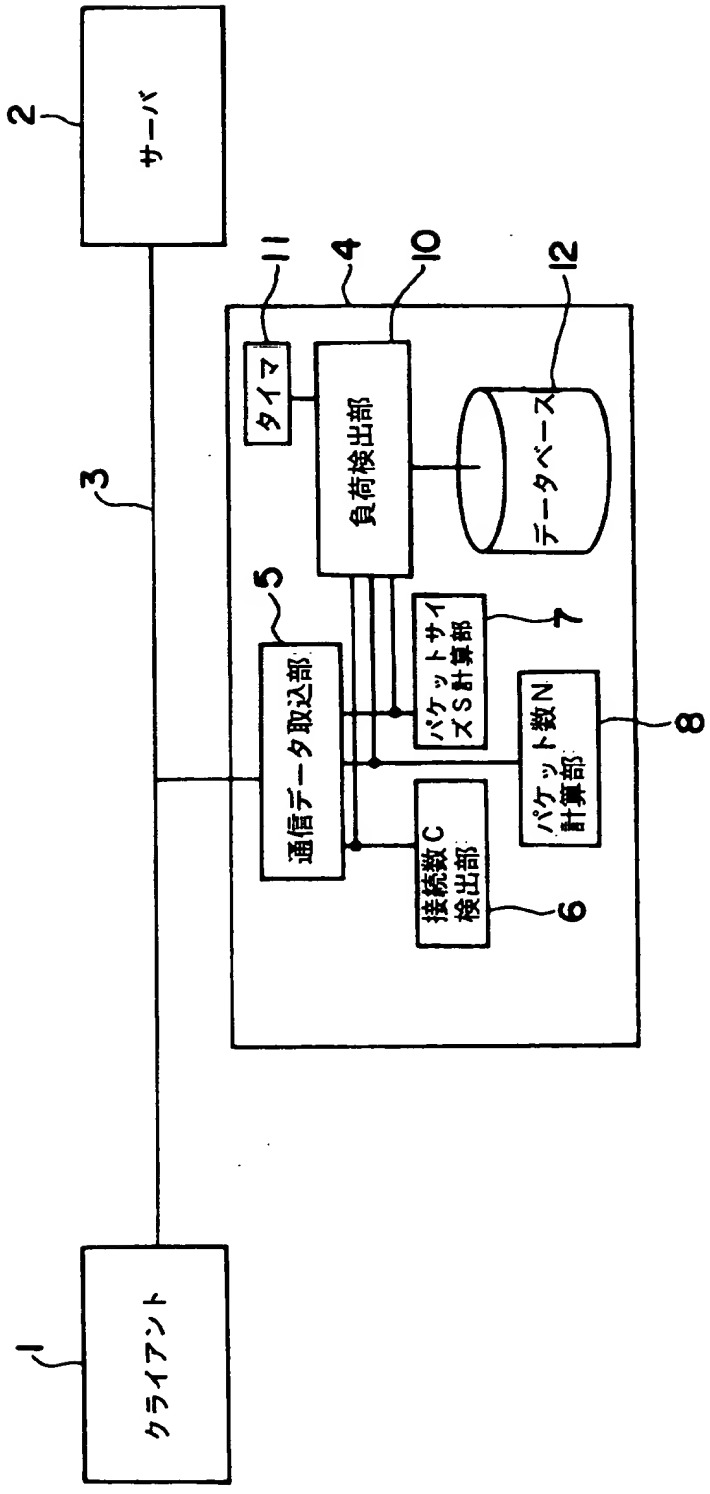
【図１４】　過去のクライアント側処理能力値の分布例を示すグラフ図

【図１５】　修正関数を説明するための図（２）

【書類名】　図面

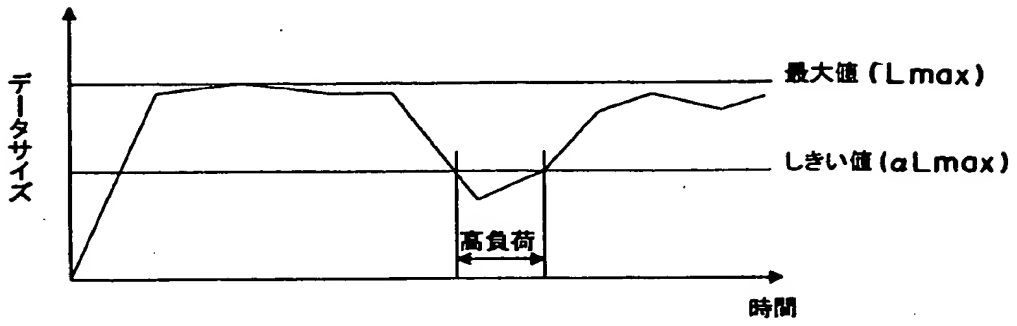
【図１】

本発明の実施形態である負荷検出装置の接続構成を示す図



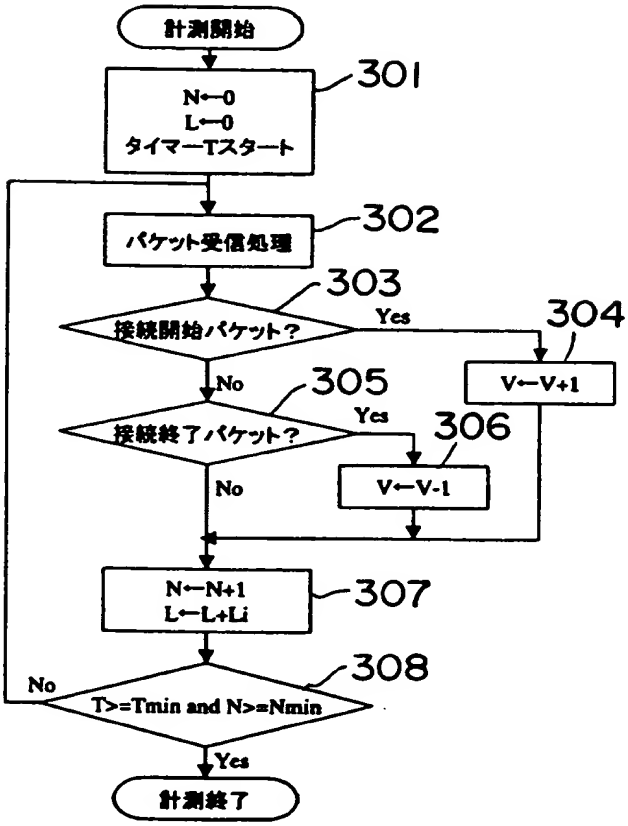
【図２】

実施形態におけるサーバの高負荷判定を行うためのデータサイズと時間との関係を示したグラフ図



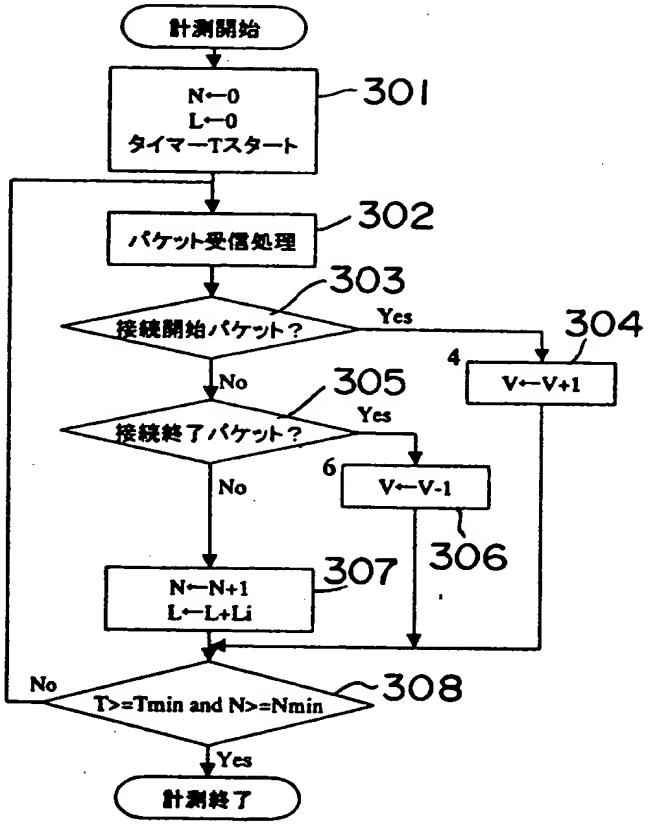
【図３】

実施例１におけるパケット監視方法を示すフロー図（１）



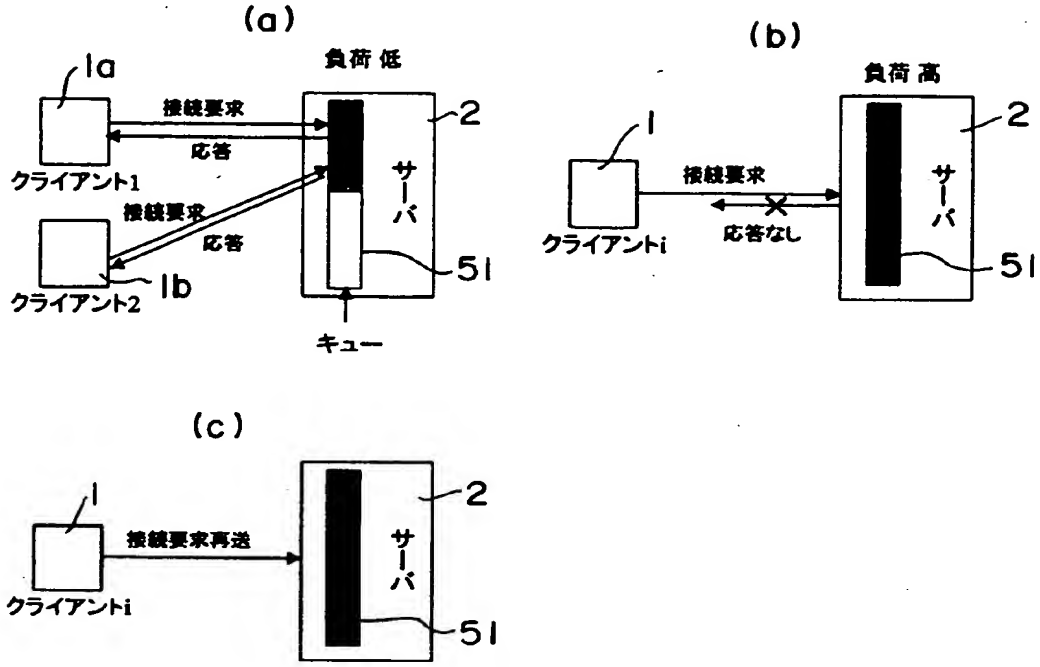
【図４】

実施例１におけるパケット監視方法を示すフロー図（２）



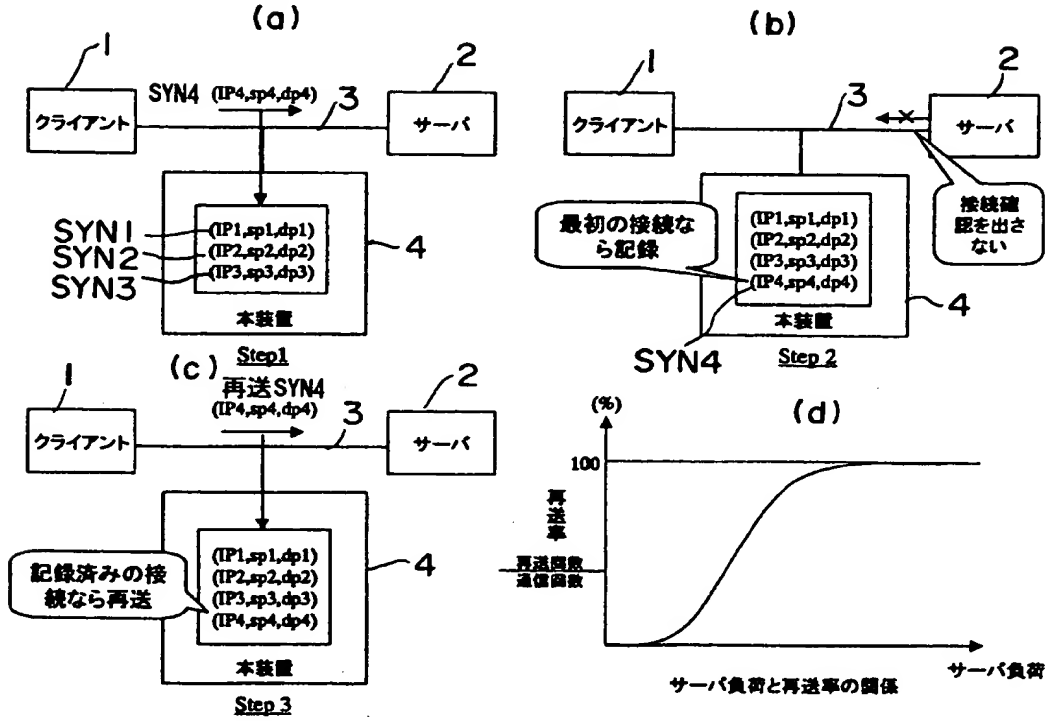
【図５】

クライアントからサーバへの接続要求と、バッファの状態に応じた応答処理を説明するための図



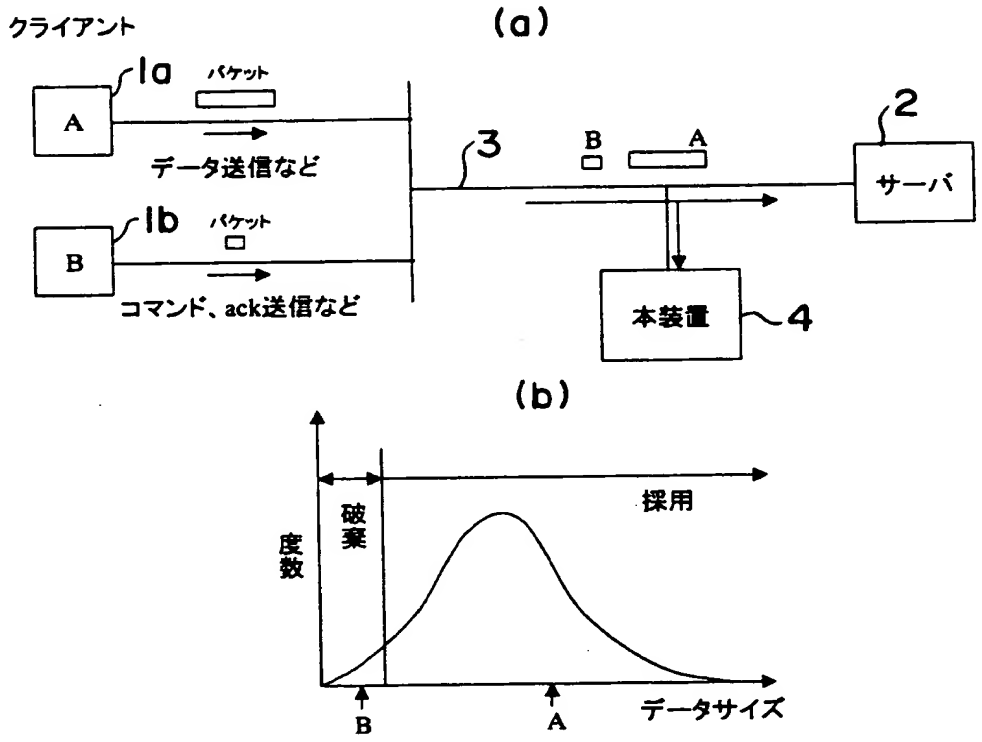
【図６】

クライアントからサーバへの接続要求の再送を説明するための図



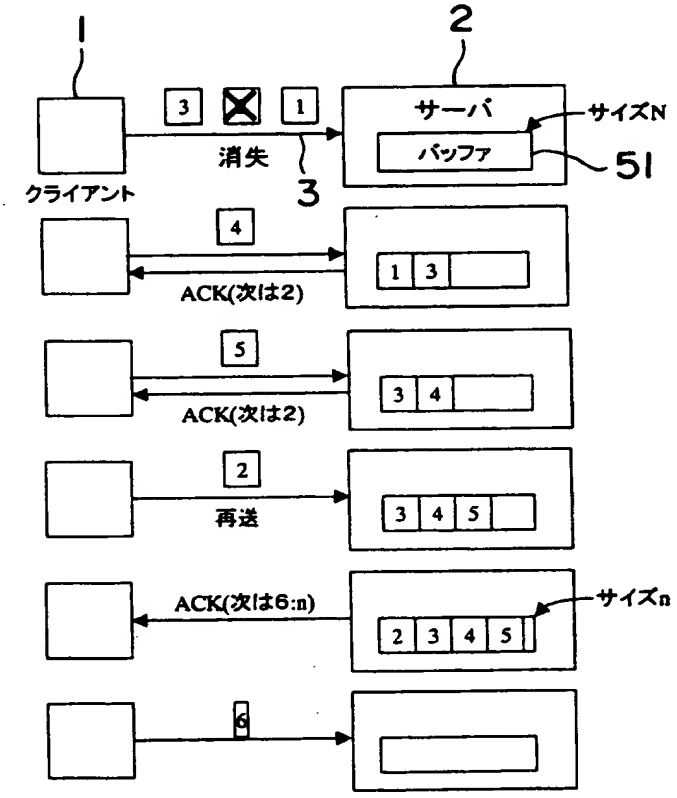
【図７】

負荷検出においてデータサイズによって対象データとするか否かの弁別を行う例を示す説明図



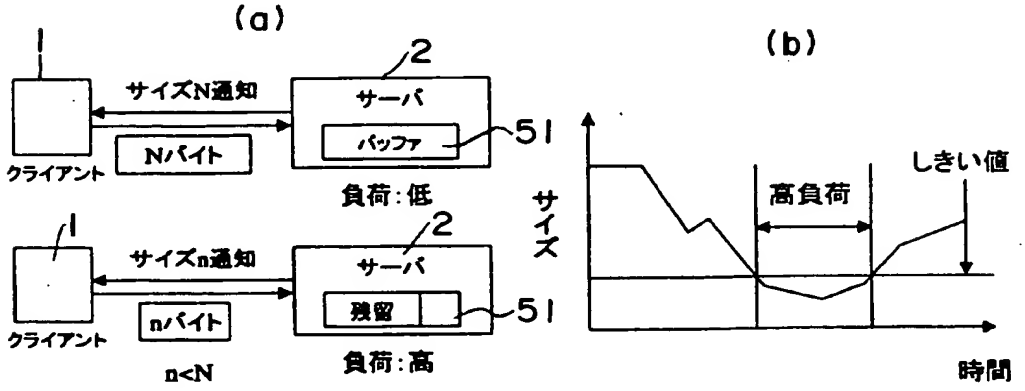
【図８】

シーケンス番号に基づくサーバの処理を説明するための図



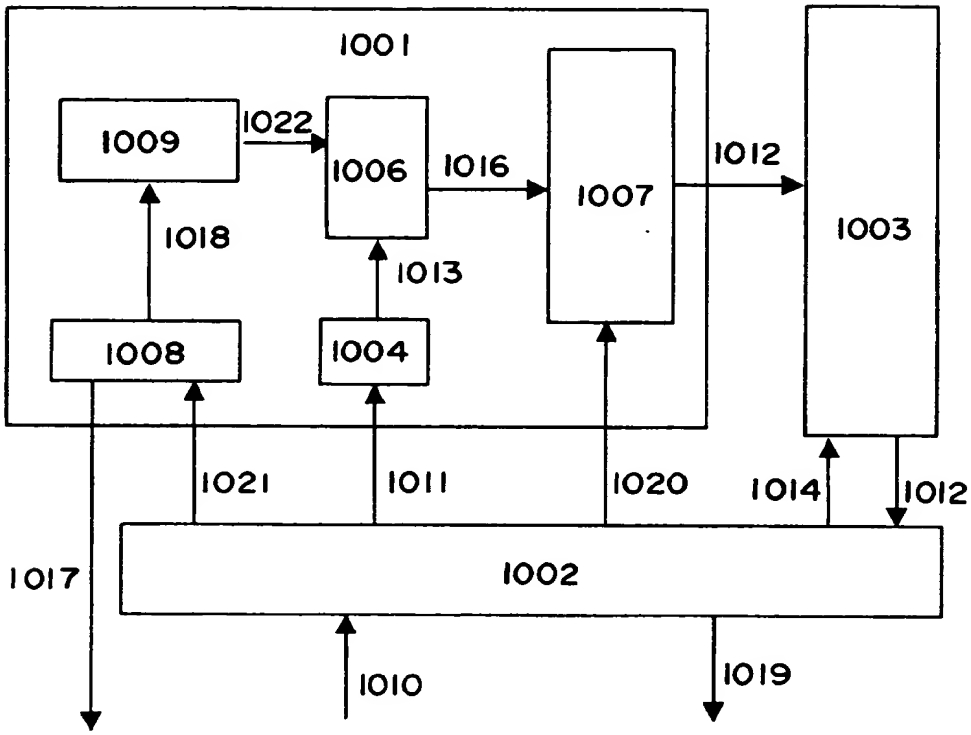

【図９】

サーバからクライアントへの通信を監視する説明図



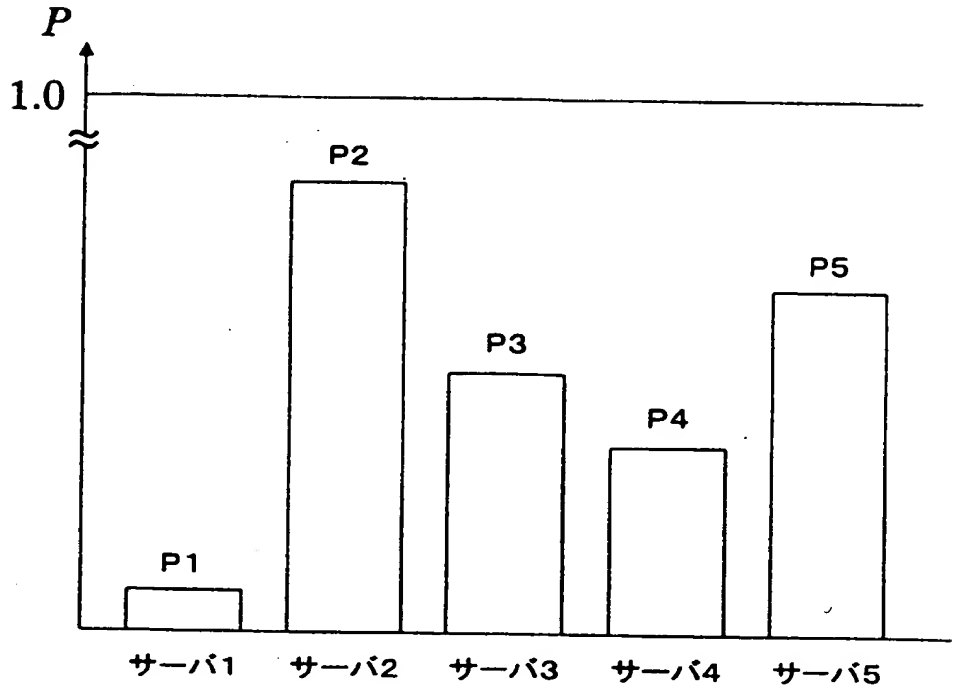
【図１０】

実施形態のサーバ割当装置の構成を示すブロック図



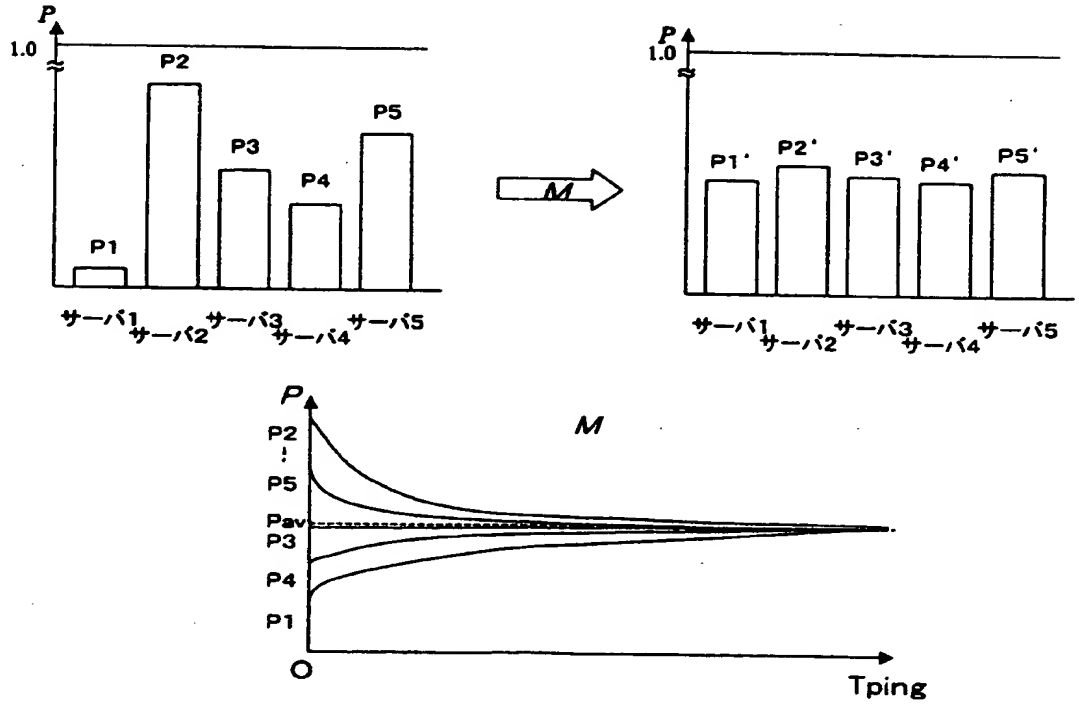
【図１１】

サーバ割当確率分布ＰｓＤを説明するためのグラフ図



【図１２】

修正関数を説明するための図（１）



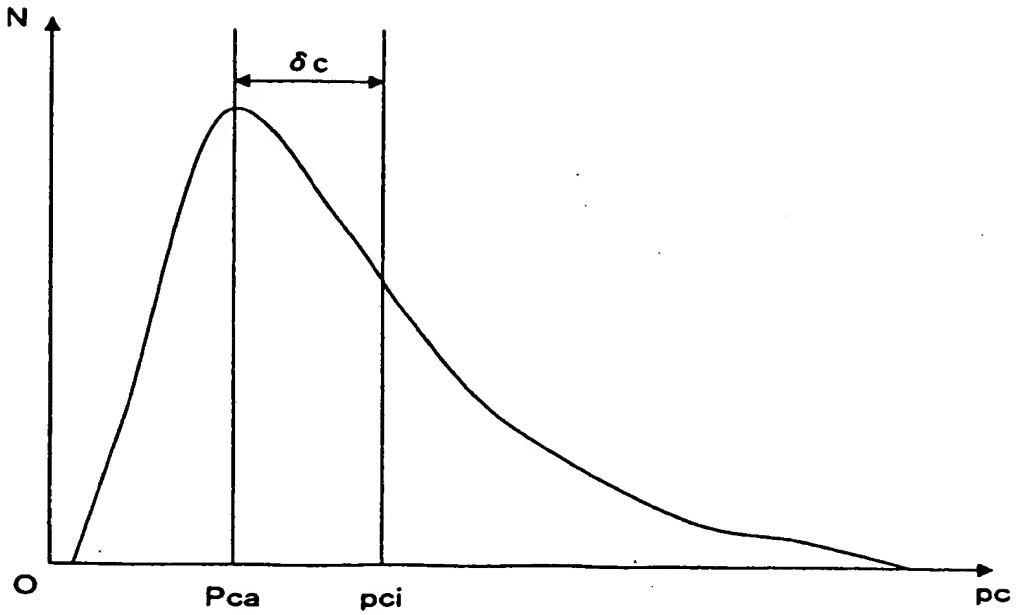

【図１３】

実施形態において、サーバ選択手段により生成されるテーブルの一例を示す図

| #0 | #1 | #2 | #3 | #4 |
|---|---|---|---|---|
| 0～0.04<br>サーバ1 | 0.05～0.34<br>サーバ2 | 0.35～0.55<br>サーバ3 | 0.56～0.80<br>サーバ4 | 0.81～1.00<br>サーバ5 |

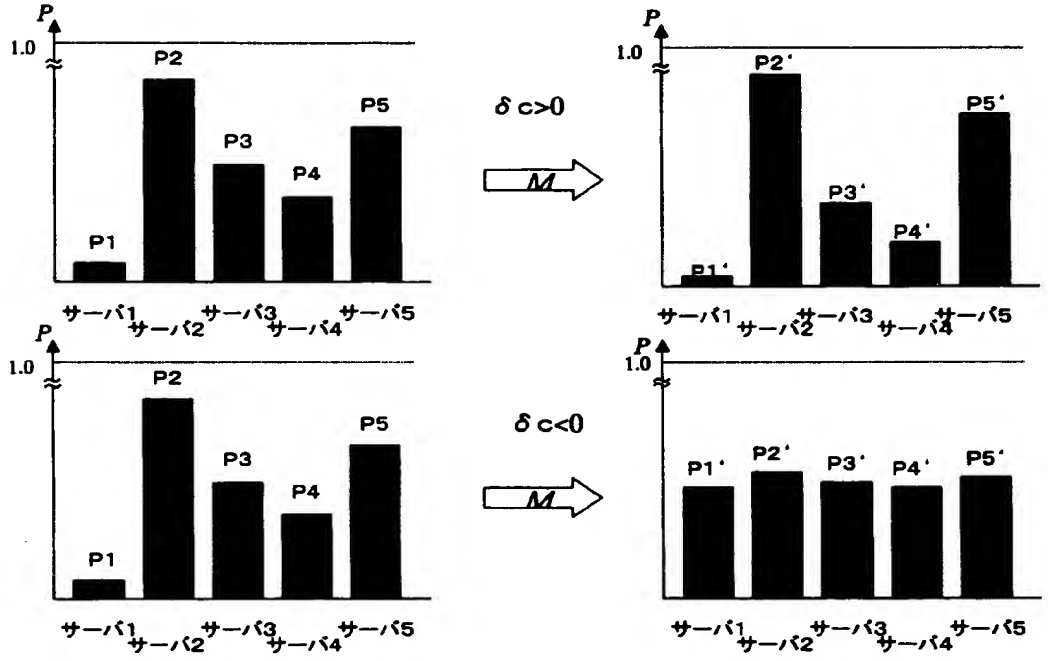
【図１４】

過去のクライアント側処理能力値の分布例を示すグラフ図



【図１５】

修正関数を説明するための図（２）



【書類名】　　要約書

【要約】

【課題】　サーバの負荷検出およびその割当を高精度かつ効率的に行う。

【解決手段】　クライアントからサーバへの通信を監視し、接続当たりの通信データサイズをサーバの負荷として計測して、接続当たりの通信データサイズの変化を検出し、最大値を記録するとともに、前記最大値に対するその時点での接続当たりの通信データサイズが小さくなればサーバが高負荷であると判断するようにした。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005223
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】　富士通株式会社
【代理人】　申請人
【識別番号】　100089244
【住所又は居所】　東京都中央区東日本橋３丁目４番１０号　ヨコヤマビル６階　秀和特許法律事務所
【氏名又は名称】　遠山　勉
【選任した代理人】
【識別番号】　100090516
【住所又は居所】　東京都中央区東日本橋３丁目４番１０号　ヨコヤマビル６階　秀和特許法律事務所
【氏名又は名称】　松倉　秀実

# 出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社